Vendor Information Security Requirements

This Exhibit supplements and is incorporated by reference into the agreement to which it is appended or in which it is referenced ("Agreement"). In the event of conflict between the terms of this Exhibit and any other terms in the Agreement or otherwise entered into by the parties that relate to the provisions set forth herein, the terms of this Exhibit shall supersede and prevail.

1. Definitions

The following terms have the meanings set forth below. Capitalized terms not otherwise defined herein shall have the meanings given in the Agreement.

1.1. "**Data Protection Laws**" means all applicable data and/or privacy laws, rules or regulations in connection with all use and processing of Protected Information including Personal Data, including laws, rules or regulations of any applicable country from which such data originated, including laws, rules or regulations that relate to the security and protection of personally-identifiable information, data privacy, trans-border data flow or data protection.

1.2. "**Data Controller**" means the entity responsible for determining the purposes and the means of Processing Personal Data. The term "Data Controller" includes entities that assume the role of "Data Controller" (e.g., under GDPR), "Business" (e.g., under CCPA / CPRA), or other analogous roles in Data Protection Laws.

1.3. "**Data Processor**" means the entity that Processes Personal Data on behalf of a Data Controller. The term "Data Processor" includes entities that assume the role of "Data Processor" (e.g., under GPDR), "Service Provider" (e.g., under CCPA / CPRA), or other analogous roles in Applicable Data Protection Laws.

1.4. "**Harmful Code**" means vulnerabilities, viruses, worms, time bombs, key-locks, Trojan horses and other malicious code, files, scripts, agents or programs that could disrupt or interfere with the operation of the Products or equipment upon which the Products or Services operate.

1.5. "**Information Systems**" means all hardware, software, networks, and associated services that relate to or enable any of the features or functionality of the Products or Services and/or that store, transmit, enable access to, or Process Protected Information. For avoidance of doubt, Information Systems includes any software Company utilizes to integrate with a Convergint-provided API.

1.6. "**Personal Data**" means information relating to an identified or identifiable natural person or information otherwise considered "personal data" or "personal information" under applicable Data Protection Laws.

1.7. "**Protected Information**" means information provided by, about, or pertaining to Convergint, information pertaining to or created by Convergint's use of the Products or Services, and information that is considered confidential to Convergint pursuant to the Agreement or that Company should understand to be confidential based on the circumstances. Protected Information also includes Personal Data.

1.8. "**Products**" means those products and services, including related documentation, that are sold or supplied, directly or indirectly, by Company to Convergint.

1.9. "**Security Incident**" means any potential, suspected, or actual unauthorized disclosure, loss, destruction, compromise, damage, alteration, access or theft of an Information System and/or Protected Information.

2. Information Security Measures

2.1. General. Company shall implement appropriate administrative, technical, physical, and organizational measures to ensure the security, confidentiality, integrity, availability, and resilience of all Information Systems, Products, Services, and Protected Information.

2.2. Governance. Company shall create, implement and maintain an enterprise information security program that governs the Information Systems, the Products, and the Services that meets or exceeds industry best practices, that meets the requirements of all Data Protection Laws, and that includes without limitation appropriate policies, governance structures, staffing, monitoring and assessment procedures. Company shall maintain and follow a reasonable and appropriate written data security policy that includes technological, physical, administrative and procedural controls to protect the confidentiality, integrity and availability of Protected Information, and that meets or exceed prevailing industry standards or an applicable third-party security assurance standard such as ISO 27001 or Statement on Standards for Attestation Engagements No. 18 Type II ("SSAE 18") (SOC 2 Type II).

2.3. Product Security and Testing. Company shall test all Products and Services prior to making them available to ensure such Products or Services do not contain Harmful Code and meet or exceed industry best practices for information security. Company shall engage qualified security representatives, either internal or external, to perform penetration, vulnerability, or other applicable forms of testing on the Products and Services at least annually.

2.4. Software Development. Company shall create, implement and maintain a secure software development lifecycle (SDLC) program that meets or exceeds industry best practices for all software, applications, or code applicable to the Products and Services, including documented secure coding standards that are referenced and followed for all development activities. Company shall evaluate and document the risk of each application security issue identified. Company shall

remediate identified application security issues utilizing a risk based approach within a reasonable timeframe in accordance with industry best practices.

2.5. System Administration. Company shall create, implement, and maintain system administration procedures for its Information Systems that meet or exceed industry best practices for information security, including without limitation, inventorying of systems, system hardening, event logging, firewall protection, malware protection, system and device patching and proper anti-virus installation and updates.

2.6. Access Controls. Company shall manage access rights to the Information Systems and Protected Information on a least privilege and need-to-know basis, including through the use of defined authority levels and job functions, and shall maintain a record of privilege levels. Company shall create, implement and maintain controls protecting access to the Information Systems and Protected Information that meet or exceed industry best practices, including at least unique user IDs, changing default passwords, multi-factor authentication, and a password policy that adopts prevailing industry standard for length, character type, complexity, expiry, re-use, and lock-outs, along with a review of user and privileged user access rights at least annually. Company shall maintain strict operating standards and guidelines for privileged user status, including but not limited to training and monitoring.

2.7. Encryption. Company shall ensure that all Protected Information is, at all times, encrypted using encryption mechanisms that meet or exceed industry standards while in transit (including but not limited to on public networks, email systems, or within Company's internal network) and while at rest (including without limitation where it is stored on servers, computers, smart phones / tablets, or removable media).

2.8. Data Segregation. Company shall create, implement, and maintain logical or physical data segregation that meets or exceeds industry standards to ensure Protected Information is not accessible by unauthorized users and not commingled with data from other end users or customers.

2.9. Logging. Company shall create, implement, and maintain security and system event logging procedures for the Information Systems, Products, and Services designed to meet or exceed industry standards in the detection, investigation and response to suspicious activity in a timely manner, including retention of event logs for at least twelve (12) months.

2.10. Patch Management. Company shall implement and maintain patch management procedures for the Information Systems, Products, and Services that meet or exceed industry best practices and that require patches to be prioritized, tested, and installed based upon criticality according to timelines that meet or exceed industry best practices. Company shall have and follow a process for identifying and disclosing known vulnerabilities related to the products or services provided to its end users or customers. Upon request, Company shall provide the status of remediation efforts for vulnerabilities determined to present material risks to the Products, Services, or Information Systems. Company shall have the relevant patch installed within seven (7) days of patch release for vulnerabilities prioritized as "Critical," within thirty (30) days of patch release for vulnerabilities prioritized as "High," and within a commercially reasonable period of time (not to exceed ninety (90) days) for all other vulnerabilities.

2.11. Network Security. Company shall create, implement and maintain internal and external network security policies and procedures for the Information Systems that meet or exceed industry best practices. Company shall implement firewalls, email and spam protection mechanisms, network segmentation, and actively monitor the Information Systems for suspicious activity.

2.12. Endpoint Security. Company shall ensure all devices used by its personnel are configured with security software including multi-factor authentication, anti-virus, anti-malware, and encryption; that each user account is associated with a specific, individual user; that each device is configured to the maximum extent possible for automatic security updates; that each device includes endpoint detection and response software and capabilities, and that each deice is configured to meet or exceed industry best practices for automatic locking, passwords, scanning for Harmful Code, and website or content filtering.

2.13. Physical Security. Company shall create, implement and maintain physical security policies and procedures for all facilities that contain or allow access to the Information Systems or Protected Information.

2.14. Testing. Company shall conduct at least quarterly vulnerability testing and annual penetration testing (both internal and external) for all the Information Systems, Products, and Services, and complete timely identification, tracking, and resolution of all findings using a risk-based approach in accordance with industry best practices. Upon request, Company shall provide a copy or summary of findings from such testing. For the avoidance of doubt, the testing conducted in accordance with this Section shall not limit Convergint's right to conduct testing as otherwise authorized by this Exhibit.

2.15. Incident Response. Company shall create, implement, and maintain cyber incident response plans and procedures and shall test such plans and procedures at least annually. Company shall make available such incident response plans, or at a minimum summary forms of such incident response plans.

2.16. Compliance. Company shall comply with its obligations pursuant to all Data Protection Laws.

2.17. Remote Access. To the extent Company accesses (including remotely accesses) any of Convergint's information systems, Company shall: (1) only access such information systems upon authorization of Convergint; (2) implement and follow technical, administrative, physical, and organizational measures sufficient to ensure that Company does not compromise the security of such information systems or the confidentiality, integrity, or availability of any Protected Information; and (3) comply with all Data Protection Laws. Company shall create, implement, and maintain remote access policies and procedures that meet or exceed industry best practices, ensure access to Convergint's information systems require multi-factor authentication, and retain logs detailing activity conducted during each session for twelve (12) months.

2.18. Assessments and Audits. Upon request at any time, in the event of a Security Incident, or where required by applicable Laws, Company shall complete any reasonable information security assessments or questionnaires submitted by Convergint. Convergint may, at its sole expense and in its sole discretion, perform a confidential audit of documentation, systems, devices, networks, and other materials reasonably necessary to demonstrate Company's compliance with this Exhibit. Such audit may be conducted directly or via an independent auditor (subject to appropriate confidentiality obligations), at Convergint's discretion. Convergint or its independent auditor may conduct vulnerability tests or pentests of the Information Systems with reasonable prior notice to Company. Company shall provide Convergint or its independent auditor assistance as reasonably necessary for initiation and performance of such audits or tests. When conducting audits, vulnerability tests, or pentests, Convergint shall comply with Company's reasonable directions to minimize disruption to Company's business and to safeguard the Information Systems and Confidential Information. Company shall in a timely fashion and consistent with industry best practices track and resolve all findings arising out of any audits, vulnerability tests, or pentests, and confirm in writing such resolutions upon request.

2.19. Incident Notification and Response. Company agrees to promptly and without undue delay (but in any event within 24 hours of becoming aware of it) notify Convergint (with a copy to dataprotectionofficer@convergint.com) of any Security Incident. Such notice shall summarize in reasonable detail the nature of the incident, the type of data that was subject to the Security Incident, the identity of each affected data subject, the effect on Convergint, if known, of the Security Incident, the corrective actions taken or to be taken by Company along with associated timelines, and any other information Convergint may reasonably request and provide sufficient information to enable Convergint to meet its obligations under Data Protection Laws. Company shall utilize best efforts and take immediate steps to investigate, contain, and mitigate the consequences of the Security Incident, including to restore the last available backup of any protected Information that may have been lost, damaged, or destroyed. Company shall promptly take such reasonable and commercial steps as requested by Convergint to cooperate in the investigation, notification, mitigation, and remediation of any Security Incident at Company's own expense.

2.20. Employee Screening. Company shall create, implement and maintain policies and procedures that meet or exceed industry best practices regarding the background screening of all Company personnel, including without limitation and to the extent permitted by applicable law a criminal history screening that covers a period of seven (7) years. To the extent Company provides professional services Convergint, Company shall comply with reasonable requirements for background screening of Company personnel. Company shall ensure its personnel's access to the Information Systems and Protected Information is revoked immediately upon termination or when access is no longer required.

2.21. Training. Company shall create, implement and maintain a security awareness program for Company Personnel, which provides initial education and on-going awareness on at least an annual basis of information security best practices, privacy compliance, incident notification procedures, and adherence to Company's information security policies.

2.22. Business Continuity. Company shall create, implement, and maintain business continuity and disaster recovery plans (including creation of ongoing backups of applicable Information Systems) that meet or exceed industry best practices to enable prompt recovery of all Information Systems and Protected Information in the event of an unforeseen outage. Upon request, Company shall make such plans (or summaries of such plans) available to Convergint. Company shall implement its business continuity and disaster recovery plans as required to ensure Company continues to function through an operation interruption, and: (i) continues to provide the Services within 24 hours (RTO); and (ii) maintains data that is no less than 8 hours from point of outage (RPO). Company shall test business continuity and disaster recovery plans on at least an annual basis to determine the effectiveness of the plan and the organizational readiness to execute the plan.

2.23. Backups. Company shall maintain backup plans, procedures, and infrastructure to ensure that Company can quickly and efficiently restore compromised or disabled Information Systems, including availability and access to all associated Protected Information.

2.24. Data Destruction. Company shall destroy or return Protected Information to Convergint subsequent to the term of this Agreement and applicable retention periods. Destruction shall be carried out in accordance with industry best practices.

2.25. Service Providers / Subcontractors. If Company utilizes service providers or subcontractors in its provisioning of Products or Services, Company shall: (a) obtain Convergint's express, written permission; and (b) shall ensure such service providers or subcontractors comply with all provisions of this Exhibit. Company shall be liable for any failure of its service providers or subcontractors to comply with all provisions of this Exhibit.

2.26. Cloud. Where Company is leveraging cloud-based services, Company shall ensure its cloud service provider maintains at all times an up-to-date certification under ISO 27001 or can provide an up-to-date, unqualified SOC 2 Type II report, in each case dated within the past 12 months. Company shall create, implement, and maintain security practices which meet or exceed industry best practices governing the information security of the cloud services utilized. Company shall create, implement and maintain a formal program to track and report end users with access to cloud systems that support the Products and Services. Company shall gain appropriate assessment rights at any utilized cloud service provider sufficient to allow Convergint to audit the cloud platform. For any cloud service providers that will not agree to assessment rights, Company shall ensure that appropriate independent audit testing occurs annually and the resulting reports (e.g. SSAE 16 SOC2, ISO 27001, etc.) are reviewed and subsequently shared with Converging upon request. Company shall maintain all Protected Information in the original country of origin absent express authorization from Convergint (as applicable). Company shall establish controls to know the location of all Protected Information at all times.

2.27. BCRP. Company shall maintain a Business Continuity and Resiliency Plan ("BCRP") that includes procedures for disaster recovery which are adequate to ensure continuity of operation of Company's business processes (or the business processes of any third party on whom Company relies) so as to ensure that there is no disruption to all or any part of its business which would cause Company not to be able to perform its duties and obligations under this Agreement. Company shall provide the BCRP to Convergint for review upon Convergint's request. Should Convergint deem the BCRP to be inadequate for any reason, including, but not limited to, the intended use of the Products, Company shall, at its own expense, work with Convergint to amend its BCRP and implement such changes as are necessary to ensure its adequacy.

3. **Reseller provisions**. To the extent that Convergint will be reselling, distributing, or otherwise making available Company's products or services to End Users (defined below), the following additional provisions shall apply.

3.1. **Definitions**:

3.1.1. "**End User**" means the final purchaser or customer that has acquired Products or Services from Convergint.

3.1.2. "**End User Data**" means any information and data, or any derivatives thereof, concerning End Users and/or their use of the Products or Services, collected by Company or Convergint, including information and data stored by End Users in the Products. End User Personal Data is a subset of End User Data and includes all data for which End User is a Data Controller. End User Data shall be and remain the sole and exclusive property of End User.

3.1.3. "**Personal Data**," for avoidance of doubt, includes any personally identifiable information relating to any End Users or its officers, directors, employees, agents, subcontractors or customers, as well as Personal Data for which End User is a Data Controller.

3.1.4. "**Protected Information**" further includes End User Data.

3.2. For all obligations under this Exhibit under which Company is obligated to provide documents, information, materials, assistance, cooperation, or other rights to Convergint, Company agrees to provide such documents, information, materials, assistance, cooperation, or other rights to End Users, but solely to the extent relevant to such End User. Company shall reasonably cooperate with Convergint to enable Convergint to meet its contractual obligations to End Users.

3.3. Company shall comply with all privacy, data protection, or information security instructions or policies of End Users, including any associated information security requirements and, to the extent Company provides professional services to an End User, those pertaining to background screening of personnel. To the extent Company or its Information Systems Process any End User Personal Data, Company shall comply with any applicable data processing addendums agreed to with the End User. Company shall ensure its personnel's access to the Information Systems or End User's information systems is revoked immediately upon termination or when access is no longer required.

3.4. Company shall provide Convergint and End Users with prompt disclosure of material vulnerabilities and recommended patching or remediation guidance. Hardening guides for Products shall be furnished upon request.

3.5. To the extent Company accesses (including remotely accesses) any of End User's information systems, Company shall: (1) only access such information systems upon authorization of Convergint or End User (as applicable); (2) implement and follow technical, administrative, physical, and organizational measures sufficient to ensure that Company does not compromise the security of such information systems or the confidentiality, integrity, or availability of any Protected Information; and (3) comply with all Data Protection Laws. Company shall create, implement, and maintain remote access policies and procedures that meet or exceed industry best practices, ensure access to End User's information systems require multi-factor authentication, and retain logs detailing activity conducted during each session for twelve (12) months

3.6. In the event of a Security Incident, Company shall, as part of its initial notification or as soon thereafter as possible, provide Convergint with an identification of impacted End Users. Company shall further provide Convergint with all cooperation necessary to allow Convergint to meet the requirements of its agreements with End Users, and provide End Users with all notifications and cooperation to allow End Users to meet their obligations under Data Protection Laws.